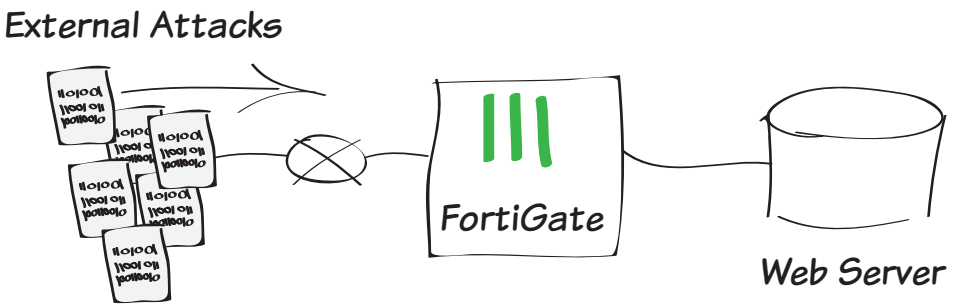
Protecting a web server from common external attacks

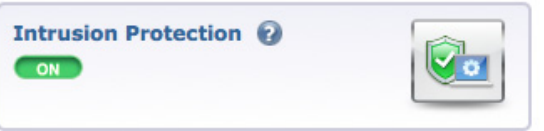
In this example, you will protect a web server using an Intrusion Prevention System (IPS) profile and a Denial of Service (DoS) policy. This will prevent a variety of different attacks from reaching the server.

1. Enabling Intrusion Protection
2. Configuring the default IPS profile to block common attacks
3. Adding the IPS sensor to the server access security policy
4. Creating a DoS policy
5. Results



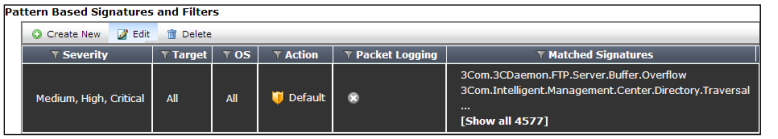
1. Enabling Intrusion Protection

Go to **System > Config > Features** and ensure that **Intrusion Protection** is turned **ON**. Apply your changes if necessary.

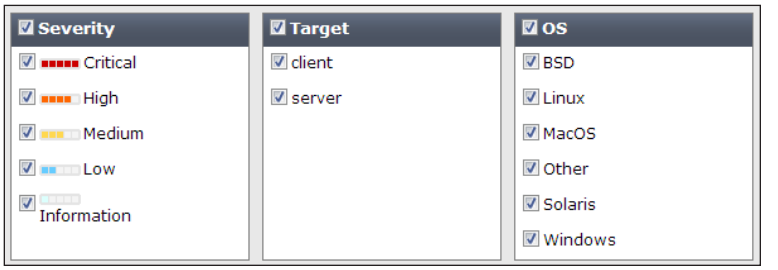


2. Configuring the default IPS profile to block common attacks

Go to **Security Profiles > Intrusion Protection** and edit the **default** profile. In the **Pattern Based Signatures and Filters** list, highlight the default entry and select **Edit**.



Select **Severity** to view all signatures in the database.



Scroll down and set the **Action** to **Block All**.

Enable all the listed **Rate Based Signatures**.

Rate Based Signatures

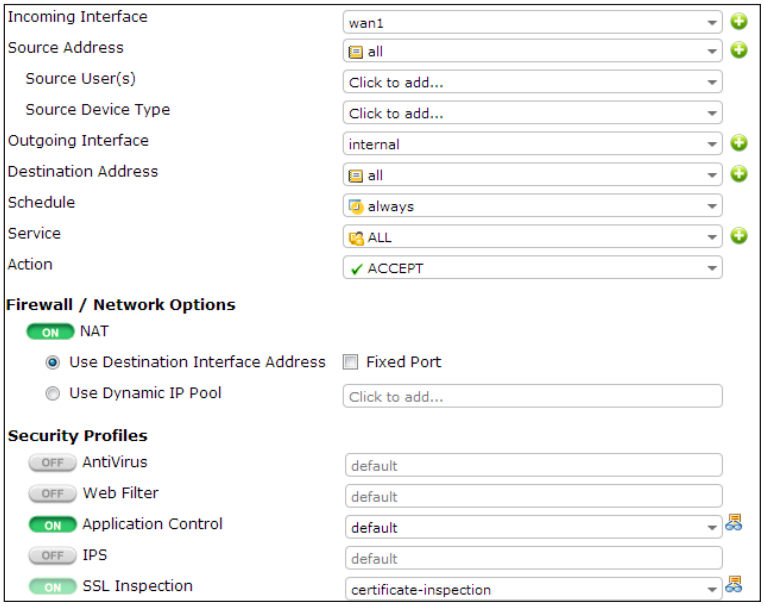
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes
ON	Apache.HTTP.Server.Range.DoS	30	1	Any	Block	0
ON	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	0
ON	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	0
ON	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	0
ON	FTP.Login.Brute.Force	200	10	Any	Block	0
ON	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	0
ON	IMAP.Login.Brute.Force	60	10	Any	Block	0
ON	Lotus.Domino.Login.Brute.Force	300	10	Any	Block	0
ON	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	0
ON	MS.RDP.Connection.Brute.Force	200	10	Any	Block	0
ON	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	Block	0
ON	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	Block	0
ON	MS.XML.Core.Services.Memory.Corruption	5	10	Any	Block	0
ON	MySQL.Login.Brute.Force	60	60	Any	Block	0
ON	Novell.Open.Enterprise.Server.HTTPSTK.DoS	19	1	Any	Block	0
ON	POP3.Login.Brute.Force	200	10	Any	Block	0
ON	SMB.Login.Brute.Force	500	60	Any	Block	0
ON	SSH.Connection.Brute.Force	200	10	Any	Block	0
ON	Telnet.Login.Brute.Force	60	60	Any	Block	0
ON	Wordpress.Login.Brute.Force	1000	10	Any	Block	0

3. Adding the IPS sensor to the server access security policy

Go to **Policy & Objects > Policy > IPv4** and edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** under **Security Profiles** and set it to use the **default** profile.

Enabling IPS automatically enables **SSL Inspection**. Set this feature to use the **certificate-inspection** profile.

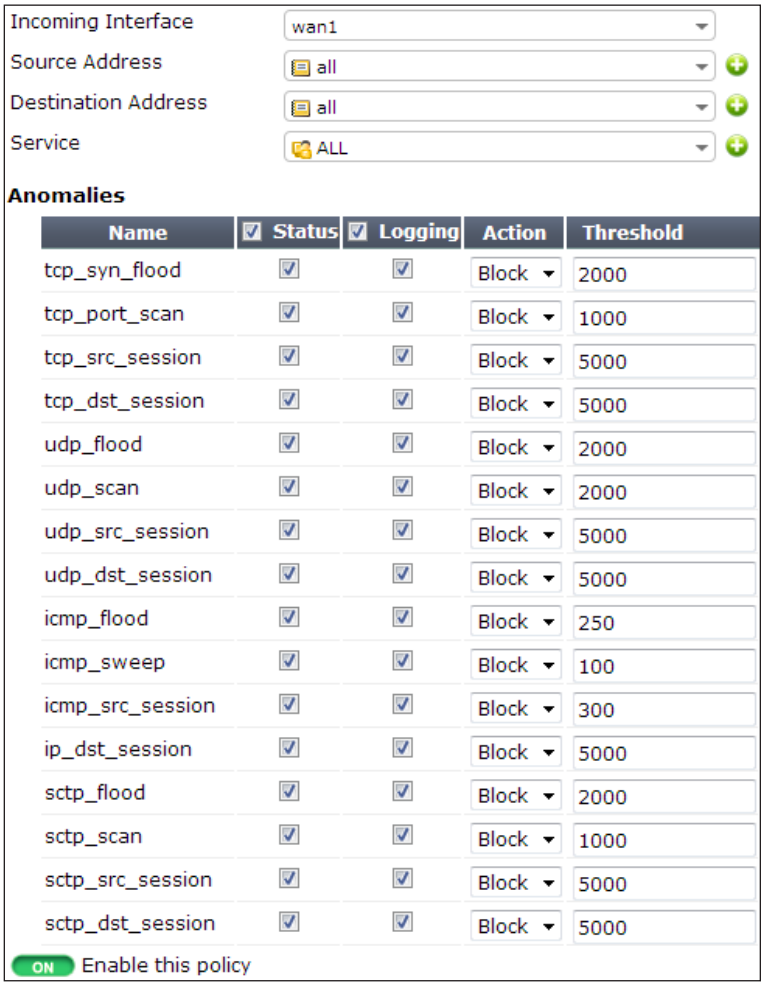


4. Creating a DoS policy

Go to **Policy & Objects > Policy > DoS** and create a new policy.

Set **Incoming Interface** to your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.



5. Results

DoS attacks are illegal, unless you own the server under attack. Before performing an attack, ensure that you have the correct server IP.

Launch a DoS attack on your web server's IP address.

Go to **System > FortiView > Threats** and select the **5 Minutes** view.

You will see that a DoS attack has been detected and blocked.